

[NT] Kerio Personal Firewall Denial of Service Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0100.html>

From: support@securiteam.com

Date: 08/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 26 Aug 2002 21:34:03 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Kerio Personal Firewall Denial of Service Vulnerability

SUMMARY

Kerio Personal Firewall (KPF) is a software agent that builds a barrier between your personal computer and the Internet. KPF is designed to protect your PC against attacks from both the Internet, and other computers in the local network.

Kerio Personal Firewall 2.x.x for the Windows platform contains a Denial of Service vulnerability. This vulnerability allows an attacker to cause the host to hang-up and to cause its CPU utilization to jump to 100%.

DETAILS

Vulnerable systems:

* Kerio Personal Firewall version 2.x.x

1] DoS vulnerability with Kerio Personal Firewall 2.x.x Default Installation

-- KPF is vulnerable to a Synflood attack. By sending the host a minimum of 300 SYN packets, it is possible to cause the attacked host to no longer respond, and to cause its CPU utilization to reach 100%.

Securiteam: [NT] Kerio Personal Firewall Denial of Service Vulnerability

2] Setting the Personal firewall to High Security and Block all services and Protocols

– It is quite similar to the first one but here the personal firewall is configured to block all its offered services and protocols. After sending a minimum of 500 SYN packets to the port range of 1–1024, the host will no longer respond and 100% of the CPU time will be consumed.

ADDITIONAL INFORMATION

The information has been provided by <mailto:sunninja@scientist.com>
Abraham Lincoln.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NT] Multiple OmniHTTPd Issues (CSS)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)